REMARKS

Claims 1 and 3-21 were pending and stand rejected. Claims 1, 3, 4, 6, 7, 10, 11, 13, 14 16, 18, 19, and 20 are amended. Claims 5, 12, and 17 are canceled. Claims 22-24 are newly added. Claims 1, 3, 4, 6-11, 13-16, and 18-25 are pending upon entry of this amendment.

Objection to the Specification

The specification stands objected to for typographical errors as well as for failing to follow certain formalities. Applicants have amended page 7, line 7 of the specification as suggested by the Examiner.

The Examiner also requested that page 7, line 26 of the specification be amended to read "command" instead of "commend". Applicants note that this portion of the specification does not contain the typographical error suggested by the Examiner.

Objection to the Claims

Claim 10 is objected to for failing to end with a period. Applicants have amended claim 10 as suggested by the Examiner.

35 USC § 101 Rejections

Claims 20 stands rejected under 35 U.S.C. § 101 because the claimed invention is allegedly directed to non-statutory subject matter. Applicants respectfully traverse this rejection as applied to the amended claim.

Claim 20, as amended, recites, *inter alia*:

> A computer-readable storage medium storing computer-executable program code

Support for amended claim 20 is found throughout the specification, including at page 2, last paragraph.

Applicants note that computer program products stored on computer readable media are well-established as statutory subject matter. MPEP 2106. Accordingly, Applicants respectfully submit that amended claim 20 recites statutory subject matter and request that the Examiner withdraw the § 101 rejection of claim 20.

35 USC § 112 Rejections

Claims 3, 4, 6, and 11 stand rejected under 35 U.S.C. § 112 for indefiniteness. Applicants respectfully traverse these rejections as applied to the amended claims.

Applicants have amended claims 3, 4, 6, and 11 as suggested by the Examiner. Accordingly, Applicants respectfully submit that amended claims 3, 4, 6, and 11 are not indefinite and therefore request that the Examiner withdraw the §112 rejections of these claims.

35 USC § 103 Rejections

Claims 1 and 3-21 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Applicant admitted prior art, in view of Ramarao (U.S. Publication No. 2004/0199647), and further in view of Gruper (U.S. Patent No. 7,047,369). Applicants respectfully traverse these rejections as applied to the amended claims.

Independents claims 1, 16, and 20 recite elements related to training a database intrusion detection system. For example, independent claim 1 recites:

> observing, in real time, commands that are accessing the database during a training phase; and
> **grouping** the commands into categories;
> performing a **statistical analysis** of the categories;
> deriving from said commands, in real time, a set of acceptable commands; and

ending the training phase responsive to the statistical analysis.

The amended claims recite observing commands that are accessing the database during a training phase. **The commands are grouped into categories**. A **statistical analysis** of the categories is performed. A set of acceptable commands is derived. **The training phase is then ended responsive to the statistical analysis**. Amended independent claims 16 and 20 recite similar limitations. Support for the amendments is found throughout the specification, including at pages 13 and 14. Limiting the duration of the training phase in the claimed manner beneficially enables observation of a representative sample of acceptable commands while limiting negative consequences that might result should the training phase last too long.

The Gruper reference does not disclose or suggest "performing a **statistical analysis** of the categories" and "**ending the training phase responsive to the statistical analysis**" as recited by independent claims 1, 16, and 20. Gruper instead describes an operating environment in which application activities are defined as acceptable activities and/or suspect activities so that unacceptable application behavior can be prevented. Abstract.

However, Gruper does not disclose or suggest "performing a **statistical analysis** of the categories" and "**ending the training phase responsive to the statistical analysis**" as recited by independent claims 1, 16, and 20. The "statistical analysis" feature was previously recited in now-canceled claim 5. In rejecting claim 5, the Examiner argued that Gruper discloses a statistical analysis at column 5, lines 32-61. This portion of the reference merely discloses an operating environment featuring a learn mode. When the learn mode is activated the operating environment assigns access rights to various applications based on the observed behavior of each application. There is no disclosure,

however, of performing a statistical analysis of observed behavior during the learn mode or ending learn mode responsive to a statistical analysis. While Gruper discloses that the duration of learn mode can be configured to either run continuously or for a specific session, Gruper does not teach or suggest using statistical techniques to influence the duration of the learn mode. Thus, Gruper does not disclose or suggest "performing a **statistical analysis** of the categories" and "**ending the training phase responsive to the statistical analysis**" as recited by independent claims 1, 16, and 20.

Furthermore, Gruper also does not disclose or suggest "**grouping** the commands into categories" as recited by independent claims 1, 16, and 20, or "**grouping the commands responsive to the commands' canonical forms**" as recited by independent claim 21. The Examiner argued that Gruper discloses a "grouping" at column 5, lines 32-61. However, as indicated above, this portion of the reference merely describes an operating environment featuring a learn mode. While Gruper discloses generating an "enforcement file" during the learn mode, this file merely contains "access rights" for the various applications. Gruper, column 5, lines 34-37. Thus, Gruper does not disclose or suggest "**grouping** the commands into categories" as recited by independent claims 1, 16, and 20 or "**grouping the commands responsive to the commands' canonical forms**" as recited by independent claim 21.

The Ramarao reference does not remedy the deficiencies of the Gruper. Ramarao discloses a software environment in which a message requesting action is received from a node. A determination is made that the message is not permitted in the software environment and the message requesting action is prevented from occurring. Abstract. However, Ramarao does not disclose or suggest the "statistical analysis" recited by

independent claims 1, 16, and 20, or the "grouping" recited by independent claims 1, 16, 20, and 21.

The Applicant admitted prior art does not remedy the deficiencies of the cited references. The Applicant admitted prior art merely describes the use of real time training of a database. However, the Applicant admitted prior art does not disclose or suggest "statistical analysis" or "grouping" as claimed.

Accordingly, Applicants respectfully submit that the cited references do not teach or suggest every element of independent claims 1, 16, 20, and 21. Therefore, a person of ordinary skill in the art would considering the references either individually or in combination would not find the claimed invention obvious. The dependent claims not mentioned above incorporate the elements of their base claims and are therefore not obvious for at least the same reasons.

CONCLUSION

Should the Examiner wish to discuss the above amendments and remarks, or if the Examiner believes that for any reason direct contact with Applicant's representative would help to advance the prosecution of this case to finality, the Examiner is invited to telephone the undersigned at the number given below.

Respectfully submitted,

CAREY NACHENBERG ET AL.

Dated: May 8, 2008

By: /Brian Hoffman/
Brian M. Hoffman, Reg. No. 39, 713
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (415) 875-2484
Fax: (415) 281-1350